International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN (P): 2249–6831; ISSN (E): 2249–7943
Vol. 12, Issue 1, Jun 2022, 41–46

PROCESS-ORIENTED APPROACH FOR SECURITY METRIC – A PROPOSAL FOR SECURITY EVALUATION MODEL

SUGANTHY A

Pondicherry University, Pondicherry, India

ABSTRACT

Security is a major concern in today's digital world. With the improvements in the technology, the issues related to security raises proportionally. A number of security mechanisms are available for the developers to incorporate in their developing applications. But the authenticity and reliability of such techniques is questionable. This leads to the research in security metrics. Extensive research in security metrics are available for the research community to do their research in security metrics. But security metrics pertaining to banking applications are negligible. This paper presents the process involved in security metrics for banking applications. This paper identifies the process involved in identifying the security evaluation model. The proposed model is evaluated with the help of a case study related to online banking applications and the result shows that the proposed model provides the required level of security for the chosen application.

KEYWORDS: Security Metrics, Information Security & Process-Oriented Model

Received: Nov 23, 2021; **Accepted**: Dec 13, 2021; **Published**: Feb 02, 2022; **Paper Id**: IJCSEITRJUN20225

Original Article

1. INTRODUCTION

Information security is a major issue in the internet world. As major proportions of the applications that we use today are internet based it is necessary to take care of the security of the information that we use. The loss due to the lack of security concern for the financial applications is very huge and sometimes unacceptable. It is, therefore, necessary to protect the data as well as the software. As with the technology improvements, the challenges that we face for protecting the data also increases. When it comes to banking applications, the need for information security is more and any breach of information security will affect the reputation of the organization.

According to the Legal Information Institute, information security is defined as the protection of information and information systems against unauthorized activities and actions. The triad of information security are: (CIA) Confidentiality, Integrity and Availability. And the other principles of information security that should be considered are Authenticity.

Confidentiality: Confidentiality of the information is to protect the information from unauthorized access. This principle maintains the secrecy of the data and reveals the information only to the authorized user. Integrity: Data Integrity means that the data should be modified only by an authorized user. Data integrity ensures the completeness and accuracy of the data. Availability: This ensures that the data should be accessible by an authorized user at any point in time. Authentication: Authentication of the system involves identifying the parties involved in the communication network.

Any system that provides information security should always include the CIA triad and other security

services like authentication, nonrepudiation etc.

Security metrics provide a degree to which the security of a given application is reliable. This paper proposes a framework by which the level of security can be evaluated. An application related to banking is considered for evaluating the proposed framework.

The remainder of this paper is structured as follows: Section 2 gives the threats related to online applications, Section 3 describes the proposed process-oriented approach for evaluating the security requirements in online applications and Section 4 concludes the paper.

2. SECURITY THREATS

With the help of technological improvements, the application users get their services in an efficient way. On the other hand, the attackers are also gaining access to the protected system with their technical skills. The attackers wanted to prove their technical knowledge that they have gained. Intrusion in financial institutions will affect the trustworthiness of the institution as well. Hence security violation needs to be properly handled.

Types of Attacks in Banking

Customers of the banks find it convenient to use the online services provided by the banks. These online services provided by the banks makes the customer feel comfortable to get their services from the place where they are located and they can also avail themselves the banking services at any time. Though online banking benefits the customers in many ways, there are certain issues or sometimes the customers are reluctant to use online banking services because of security concerns. The types of attacks that could happen in online banking can be classified as:

- Credential Stealing: The credentials of the bank customers were attacked by the attacker and the attacker tries to gain the users' credentials with the help of malicious software installed in the computer from where the customer gets the online banking services. There are other ways by which the user's credential is attacked by the attacker. Some of them are by using phishing and software like keyloggers which try to capture the credentials of the users. Additional verification such as two-factor authentication helps in eliminating these threats.
- Channel Breaking attack involves manipulating the data when intercepting the communication channel between the bank server and user [3].

3. PROPOSED PROCESS MODEL

This paper proposes a security metric process shown in Figure 1. The process identified for the security metric has four major components: planning, developing solutions, validation and taking action.

Planning Phase

The planning phase involves identifying the security requirements for the application under consideration. For Online banking, the services provided by the banks online have to be evaluated with respect to the security requirements. This process has to take the input from the regulatory bodies of banking authority, and based on the regulations given by the governing authorities, this phase should identify the other requirements. Apart from identifying the security requirements, this phase includes other activities like forming a security committee and the duties of this committee includes: identifying the right people for the metric process and forming a team, managing the team with effective communications and

identifying the technological requirements or evaluating the security requirements of the application under consideration.

The planning phase should also consider the kinds of attacks that could happen in the application. Identifying the risk is another important activity in this phase. Risk mitigation plans should be identified for the risk identified related to the application under consideration.

Other supporting activities included in this phase are identifying the scope of the planning process, setting the milestones, identifying the resources, identifying the roles and responsibilities, identifying the measurement and improvement criteria and identifying the communication link.

Develop Solutions

The second phase in the security evaluation process is developing the solutions based on the requirements identified in the previous phase. Designing the solution for the identified requirements should follow the design methodology. Once the solution for the evaluation process is created, it should be made available to all the concerned people. Other activities included in this phase are documentation, support and maintenance activities.

Validation Phase

Once the security solution is developed, the next step is to evaluate the developed solution to check whether it meets the required criteria or not. This phase involves checking the developed solution to identify the errors. The other activities included in this phase are monitoring, measuring and comparing the process with the baseline data.

Take Action

This phase involves identifying the measures for improving the design. The other activities included in this phase includes: correcting the errors identified in the validation phase, giving training to all the stakeholders and supporting them and identifying the new design with an improved solution.

The proposed process model is evaluated by choosing the online banking application and the results were evaluated. The results of the evaluation process identified the security threats involved in the online applications. The vulnerabilities of the threats have to be identified and the solution for the vulnerabilities have to be designed. The results of this process indicate the actions to be considered for improving the security measures for the online applications.

Figure 1: Security Metric Process.

4. CONCLUSIONS

This paper gives the need for security evaluation methods in online applications. The aim of this paper is to propose a process-oriented approach for evaluating the security requirements of online banking applications. As security is a major concern in today's internet environment and banking services included in financial management, security requirements are a major concern. This paper identified a four-step process model which includes: planning, solution development, validation and taking action for evaluating the security requirements. The proposed model is also evaluated for banking applications and the results of the same gives the improved solutions to be considered in the future design process.

REFERENCES

1. *Vishal R. Ambhire1, Prakash S. Teltumde, "Information Security in Banking and Financial Industry", IJCEM International Journal of Computational Engineering & Management, Vol. 14, October 2011.*
2. *Thomas Heyman, Riccardo Scandariato, Christophe Huygens, Wouter Joosen, DistriNet, "Using security patterns to combine security metrics" The Third International Conference on Availability, Reliability and Security.*
3. *Mohd Khairul Affendy Ahmad, Rayvieana Vera Rosalim, Leau Yu Beng, Tan Soo Fun, "Security Issues on Banking Systems" Mohd Khairul Affendy Ahmad et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (4), 2010, 268-272*
4. *Seyed Amin Hosseini Seno, Olfat Ganji Bidmeshk, Kimia Ghaffari, "Information Security Diagnosis in Electronic Banking" 9th International conference on E-commerce with focus on E-Business, April 2015*
5. *Erland Jonsson, Laleh Pirzadeh, "A Framework for Security Metrics Based on Operational System Attributes", work has been sponsored by the Swedish*
6. *Antti Evesti, Reijo Savola, Eila Ovaska, Jarkko Kuusijärvi, "The Design, Instantiation, and Usage of Information Security Measuring Ontology" MOPAS 2011: The Second International Conference on Models and Ontology-based Design of Protocols, Architectures and Services, Copyright (c) IARIA, 2011.*

7. *Mansoor Ahmed, Amin Anjomshoaa, Tho Manh Nguyen, A Min Tjoa, "Towards an Ontology-based Risk Assessment in Collaborative Environment Using the SemanticLIFE" Second International Conference on Availability, Reliability and Security (ARES'07)0-7695-2775-2/07 $20.00 © 2007*

8. *Bangar, Ashwini, and Swapnil Shinde. "Study and comparison of cryptographic methods for cloud security." Int J Comput Sci Eng Inf Technol Res 4.2 (2014): 205-213.*

9. *Banerjee, S. O. U. M. E. N. D. U., and S. U. N. I. L. Karforma. "Object oriented metric based analysis of space efficient LSB based steganography including compression for securing transmission of e-learning documents." International journal of mechanical and production engineering research and development (IJMPERD), ISSN (2017): 2249-6890.*

10. *Singh, Vaishali, and S. K. Pandey. "Research in cloud security: problems and prospects." International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) 3.3 (2013): 305-314.*

11. *Charan, P. I. Y. U. S. H., T. A. H. S. I. N. Usmani, and SYED HASAN Saeed. "A Comprehensive Study of Various on Demand Routing Protocols for MANETs." International Journal of Electronics and Communication Engineering 4 (2015): 1-12.*